Introduction to Separation Logic

Lectures at MGS'18

Georg Struth

on action short of strike at University of Sheffield, UK

Lecture 3: Predicate Transformers

This Lecture

- predicate transformers
- monotone predicate transformers
- local predicate transformers and the frame rule
- embedding a simple while-language

Overview

- most previous approaches to separation logic use state transformers
- and so do all integrations into proof assistants—I think
- predicate transformers are simpler to formalise
- explicit fault elements are unnecessary
- Isabelle components for lattices, fixpoints etc can be reused
- results obtained in setting of endos on complete lattices/quantales

Transformers

definition

- transformer is endofunction $\varphi : L \to L$ on complete lattice L
- transformer is isotone if $x \leq y \Rightarrow \varphi\, x \leq \varphi\, y$

lemma

$(L^L, \leq)$ with $\leq$, sups and infs extended pointwise forms complete lattice

proof

by construction of convolution algebras, L^X is sup-lattice for any set X

for standard separation logic, $*$ isn't lifted ... we consider $\circ$ instead

Transformers

proposition

for complete lattice L

1. $(L^L, \circ, \leq, id_L)$ forms near sup/inf-quantale
2. isotone transformers on L form subalgebra; a pre-sup/inf-quantale

remarks

- near quantale: $\cdot$ need not preserve sups in second argument
- pre-quantale: near quantale that satisfies
- sup/inf-quantale indicates that $\circ$ (right)preserves sups/infs
- properties like distributivity lift from L to L^L

Transformers

proof of (2)

- id, $\lambda x.0$ and $\lambda x.\top$ are isotone
- $\circ$ preserves isotonicity: if φ, ψ are isotone, then so is $\varphi \circ \psi$
- sups preserve isotonicity: if all $\varphi \in \Phi$ are isotone, then so is $\bigsqcup \Phi$
- infs preserve isotonicity: if all $\varphi \in \Phi$ are isotone, then so is $\bigsqcap \Phi$

Predicate Transformers

example

if S is PAM, then

- predicate transformers $\varphi : \mathcal{P}\, S \to \mathcal{P}\, S$ form distributive near sup/inf-quantale
- subalgebra of isotone predicate transformers on $\mathcal{P}\, S$ forms distributive pre-sup/inf-quantale
- this holds in particular for PAM S_S of statelets

Propositional Hoare Logic

specification statement

$$x \leq \varphi\, y$$

- think of it as Hoare triple $\{x\}\,\varphi\,\{y\}$ for $\varphi : L \to L$
- in context of partial correctness

proposition

rules of propositional Hoare logic (PHL) derivable over complete lattices

$$x \leq y \wedge y \leq \varphi\, z \Rightarrow x \leq \varphi\, z$$

$$y \leq z \wedge x \leq \varphi\, y \Rightarrow x \leq \varphi\, z \qquad \text{if } \varphi \text{ isotone}$$

$$x \leq \varphi\, y \wedge y \leq \psi\, z \Rightarrow x \leq (\varphi \circ \psi)\, z \qquad \text{if } \varphi \text{ isotone}$$

$$(\forall \varphi \in \Phi.\ x \leq \varphi\, y) \Rightarrow x \leq (\bigsqcap \Phi)\, y$$

loop requires some preparation

Galois Connections

definition

$\varphi : L \to L$ is lower adjoint and $\psi : L \to L$ upper adjoint of Galois connection on complete lattice L if

$$\varphi\, x \leq y \Leftrightarrow x \leq \psi\, y$$

lemma

if $\varphi : L \to L$ is lower and $\psi : L \to L$ upper adjoint of Galois connection, then

- $\varphi \circ \psi \leq id \leq \psi \circ \varphi$
- φ, ψ are isotone

types could be generalised. . .

Galois Connections

proposition

$\psi : L \to L$ is upper adjoint iff it preserves infs

proof

- suppose ψ has lower adjoint φ and let $X \subseteq L$
  - then
    $\bigsqcap \psi[X] \leq g \bigsqcap X \Leftrightarrow \varphi \bigsqcap \psi[X] \leq \bigsqcap X \Leftrightarrow \forall x \in X.\ \bigsqcap \psi[X] \leq \psi x$
  - and $\psi \bigsqcap X \leq \bigsqcap \psi[X] \Leftrightarrow \forall x \in X.\ \psi \bigsqcap X \leq g\, x \Leftarrow \forall x \in X.\ \bigsqcap X \leq x$
- suppose ψ preserves infs
  - then $\bigsqcap \{y \mid x \leq \psi\, y\} \leq y \Leftrightarrow x \leq \psi\, y$
  - hence $\varphi = \bigsqcap \{y \mid x \leq \psi\, y\}$

□

Fixpoint Fusion

theorem

if $\chi : L \to L$ is upper adjoint and $\varphi, \psi : L \to L$ are isotone, then

$$\chi \circ \varphi = \psi \circ \chi \Rightarrow \chi\,(\mathit{gfp}\,\varphi) = \mathit{gfp}\,\psi$$

proof

- $\psi(\chi(\mathit{gfp}\,\varphi)) = \chi(\varphi(\mathit{gfp}\,\varphi)) = \chi(\mathit{gfp}\,\varphi) \Rightarrow \chi(\mathit{gfp}\,\varphi) \leq \mathit{gfp}\,\psi$
- let $\chi^\flat$ be lower adjoint of χ
- then $\chi^\flat \circ \psi \leq \chi^\flat \circ \psi \circ \chi \circ \chi^\flat = \chi^\flat \circ \chi \circ \varphi \circ \chi^\flat \leq \varphi \circ \chi^\flat$
- hence $\chi^\flat(\mathit{gfp}\,\psi) \leq \varphi(\chi^\flat(\mathit{gfp}\,\psi))$
- and therefore $\chi^\flat(\mathit{gfp}\,\psi) \leq \mathit{gfp}\,\varphi$
- finally $\mathit{gfp}\,\psi \leq \chi(\mathit{gfp}\,\varphi)$

Fixpoint Fusion

lemma

$\lambda\kappa.\ \kappa\, x : L^L \to L$ is upper adjoint

proof

show that $\forall \Phi.\ (\lambda\kappa.\ \kappa\, x)(\bigsqcap \Phi) = \bigsqcap(\lambda\kappa.\kappa\, x)[\Phi]$ □

proposition

if $F : L^L \to L^L$ and $\varphi : L \to L$ are isotone, then

$$\forall \psi.\ F\, \psi = \varphi \circ \psi \ \Rightarrow\ (gfp\, F)\, x = gfp\, \varphi$$

proof

$(\lambda\kappa.\ \kappa\, x) \circ F = \varphi \circ (\lambda\kappa.\ \kappa\, x) \Rightarrow (\lambda\kappa.\ \kappa\, x)\,(gfp\, F) = gfp\, \varphi$ implies claim with fixpoint fusion □

Loop Rule

definition

for $\varphi : L \to L$

$$\varphi^\omega = gfp\,(\lambda\psi.\ id_L \sqcap \varphi \circ \psi)$$

proposition

$\varphi^\omega\, x = gfp\,(\lambda y.\ x \sqcap \varphi\, y)$ if $\varphi : L \to L$ isotone

proof

- $id_L \sqcap \varphi \circ (-) : L^L \to L^L$
- $x \sqcap \varphi(-) : L \to L$
- $\forall\psi.\ (\lambda\chi.\ id_L \sqcap \varphi \circ \chi)\,\psi = (\lambda y.\ x \sqcap \varphi\, y) \circ \psi$ thus implies claim

□

proposition tells us how gfp on pre-quantale L^L maps on lattice L

Loop Rule

theorem

for $\varphi : L \to L$ isotone, the following loop rule of PHL is derivable

$$x \leq \varphi\, x \Rightarrow x \leq \varphi^{\omega}\, x$$

lemma

if $\varphi : L \to L$ is isotone, then so is φ^{ω}

Refined Rules

definition
$[x] = \lambda y.\ x \to y$ in complete boolean algebra

lemma
$[x] : L \to L$ is isotone, if L is complete boolean algebra

proposition

1. if $\varphi, \psi : L \to L$ isotone, then the conditional rule of PHL is derivable

$$p \sqcap x \leq \varphi\, y \wedge q \sqcap x \leq \psi\, y \Rightarrow x \leq (([p] \circ \varphi) \sqcap ([q] \circ \psi))\, y$$

2. if $\varphi : L \to L$ isotone, then the while rule of PHL is derivable

$$p \sqcap x \leq \varphi\, x \Rightarrow x \leq (([p] \circ \varphi)^{\omega}) \circ [q])\, (x \sqcap q)$$

3. $([p] \circ \varphi) \sqcap ([q] \circ \psi)$ and $([p] \circ \varphi)^{\omega}) \circ [q]$ are isotone

Propositional Refinement Calculus

Morgan's specification statement

in complete lattice L

$$[x, y] = \bigsqcap \{\varphi : L \to L \mid x \leq \varphi\, y \wedge \varphi \text{ isotone}\}$$

lemma

in complete lattice L,

1. $x \leq [x, y]\, y$
2. if $\varphi : L \to L$ isotone, then $x \leq \varphi\, y \Rightarrow [x, y] \leq \varphi$
3. $[x, y]$ isotone

Propositional Refinement Calculus

proposition

the rules of the propositional refinement calculus (PRC) are derivable over complete lattices

$$
\begin{aligned}
x \leq x' \wedge y \leq y' \Rightarrow [x, y] &\leq [x', y'] \\
[x, y] &\leq [x, z] \circ [z, y] \\
[\bigsqcap X, y] &\leq \bigsqcap \{[x, y] \mid x \in X\} \\
[x, x] &\leq [x, x]^{\omega} \\
[x, y] &\leq [p] \circ [p \sqcap x, y] \sqcap [q] \circ [q \sqcap x, y] \\
[x.q \sqcap x]\, y &\leq (([p] \circ [x \sqcap p, x])^{\omega} \circ [q])\, (q \sqcap y)
\end{aligned}
$$

Relations to Predicate Transformers

relational semantics

- associate $R \subseteq S_S \times S_S$ over state space S_S with each program
- alternatively nondeterministic function (state transformer) $f_R : S \to \mathcal{P}\, S$
- this assumes partial correctness
- writing $R \subseteq X \times Y$ and $f_R : X \to \mathcal{P}\, Y$ emphasises dualities

remark

- for $R \subseteq X \times Y$ we have $f_R\, x = \{y \mid (x, y) \in R\}$
- for $f : X \to \mathcal{P}\, Y$ we have $R_f = \{(x, y) \mid y \in f\, x\}$

Relations to Predicate Transformers

predicate transformers

- $[R] : \mathcal{P}\, Y \to \mathcal{P}\, X$ defined by

$$[R]\, p = \{x \mid f_R\, x \subseteq p\}$$

- $\langle R \rangle : \mathcal{P}\, X \to \mathcal{P}\, Y$ defined by Kleisli extension of f_R

$$\langle R \rangle\, p = \bigcup \{f_R\, x \mid x \in p\}$$

lemma

1. $\langle R \rangle\, p = \{y \mid \exists x.\ (x, y) \in R \wedge x \in p\}$
2. $[R]\, p = \{x \mid \forall y.\ (x, y) \in R \to y \in p\}$

Relations to Predicate Transformers

explanation

- $[R] : \mathcal{P}\, Y \to \mathcal{P}\, X$ is
  - backward/covariant $[R; S] = [R] \circ [S]$
  - inf-preserving/conjunctive $[R](\bigcap P) = \bigcap\{[R]p \mid p \in P\}$
  - $[\bigcup_{R \in \mathcal{R}} R] = \bigcap_{R \in \mathcal{R}} [R]$
  - $[R]P$ is weakest liberal precondition of P and R
- $\langle R \rangle : \mathcal{P}\, X \to \mathcal{P}\, Y$ is
  - forward/contravariant $\langle R; S \rangle = \langle S \rangle \circ \langle R \rangle$.
  - sup-preserving/disjunctive $\langle R \rangle(\bigcup P) = \bigcup\{\langle R \rangle p \mid p \in P\}$
  - $\langle \bigcup_{R \in \mathcal{R}} R \rangle = \bigcup_{R \in \mathcal{R}} \langle R \rangle$
  - $\langle R \rangle P$ is strongest postcondition of P and R

Relations to Predicate Transformers

Galois connection

$\langle R \rangle p \subseteq q \Leftrightarrow p \subseteq [R] q$

demodalisation

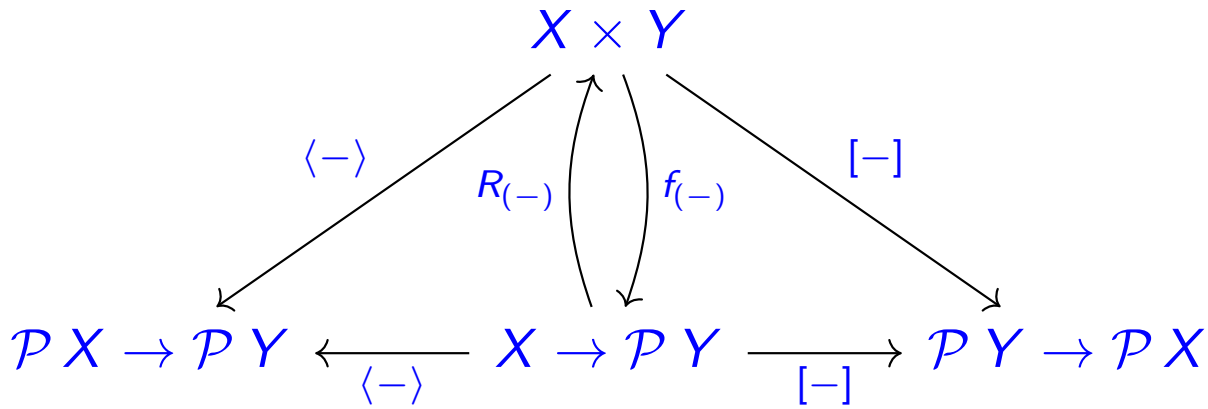
$p \subseteq [R] q \Leftrightarrow \lceil p \rceil ; R \subseteq R ; \lceil q \rceil$, where $\lceil p \rceil = \{(x, x) \mid p\, x\}$

tests (again)

- predicate transformers for conditionals/loops require those for tests
- predicates lift to (conjunctive) predicate transformers as

$$[p] = \lambda q.\ p \to q$$

Relations to Predicate Transformers



algebraic structure

- replace $X \to \mathcal{P}\,Y$ by Kleisli category of powerset functor
- replace $\mathcal{P}\,X \to \mathcal{P}\,Y$ by category of sup-lattices and sup-preserving functions
- replace $\mathcal{P}\,Y \to \mathcal{P}\,X$ by opposite of category of inf- lattices and inf-preserving functions

Predicate Transformers

summary

- studied in general setting of isotone endos over complete lattices
- PHL and PRC derivable in this setting
- conjunctive/disjunctive transformers arise as instances
- predicate transformers over assertion algebras of separation logic arise as instances
- frame rules of separation logic remains to be derived
- link with update functions of separation logic needs to be established

Locality

- isotone/conjunctive predicate transformers too weak to prove the frame rule of separation logic
- this requires local isotone transformers
- and transition from lattices to quantales

Locality

definition

if Q is quantale and $p \in Q$, then

- $\varphi : Q \to Q$ is p-local if

$$\forall q \in Q.\ p \cdot \varphi\, q \leq \varphi\,(p \cdot q)$$

- φ is local if it is p-local for all $p \in Q$

instance

- p-local predicate transformers $\varphi : \mathcal{P}\, S \to \mathcal{P}\, S$ over PAM S satisfy $p * \varphi\, q \leq \varphi\,(p * q)$
- in classical definition, p-dependency instantiated to condition
  - φ may not modify variables free in p
- in previous algebraic approaches, locality is used

Frame Rule

lemma

if Q is quantale and $p \in Q$, then $\varphi : Q \to Q$ is p-local iff frame rule holds:

$$\forall q, r.\ q \leq \varphi\, r \Rightarrow p \cdot q \leq \varphi\,(p \cdot r)$$

this doesn't require isotonicity!

Local Transformers

lemma

subalgebras of p-local quantale transformers form near-quantales

- $\lambda x.0$, id and $\lambda x.\top$ are p-local
- infs and sups of p-local transformers are p-local
- if φ is isotone and φ, ψ are p-local, then so is $\varphi \circ \psi$

theorem

subalgebras of p-local isotone quantale transformers form pre-quantales

- composition of p-local isotone transformers is p-local isotone
- fixpoints of p-local isotone transformers are p-local isotone

Local Transformers

lemma

if $\varphi : Q \to Q$ is transformer, then

1. if φ is p-local and q-local, then it is $p \cdot q$-local
2. if φ is q-local and $p \multimap q$ holds, then it is p-local

what about tests?

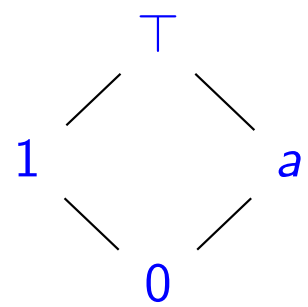
Locality of Tests

lemma

predicate transformers $[q] : Q \to Q$ need not be p-local

proof

in boolean abelian quantale defined by



$\cdot$	0	1	a	$\top$
0	0	0	0	0
1	0	1	a	$\top$
a	0	a	a	a
$\top$	0	$\top$	a	$\top$

we calculate $\top \cdot (a \to 0) = \top \cdot 1 = \top \neq 1 = a \to 0 = a \to (\top \cdot 0)$ $\square$

Locality of Tests

definition

if Q is boolean quantale and $p \in Q$, then $q \in Q$ is p-local if $p \cdot -q \leq -q$

lemma

if Q is boolean quantale and $p \in Q$, then $q \in Q$ is p-local iff
$[q] : Q \to Q$ is p-local

Locality of Tests

lemma

if S is PAM and $p, q \in \mathcal{P}\, S$ are predicates, then

1. q is p-local iff $D\, x\, y \wedge p\, y \wedge q\, (x \oplus y) \Rightarrow q\, x$
2. q is p-local iff $x \preceq y \wedge p\, x \wedge q\, y \Rightarrow q\, (y \ominus x)$, when S cancellative

example

in PAM S_S of statelets

- $q \in \mathcal{P}\, S_S$ is p-local iff

$$\forall \sigma, \eta_1, \eta_2.\ \eta_1 \preceq \eta_2 \wedge p\, (\sigma, \eta_1) \wedge q\, (\sigma, \eta_2) \Rightarrow q\, (\sigma, \eta_2 \ominus \eta_1)$$

- if q holds of a statelet and p of a piece, then q must hold of the remaining piece

Embedding a Simple Programming Language

definition

- simple while-language

$$C_B ::= x := e \mid x := *e \mid *x := e \mid x := \text{alloc}\, e \mid \text{dispose}\, e,$$
$$C ::= \text{abort} \mid \text{skip} \mid C_B$$
$$\mid C_1; C_2 \mid \text{if } p \text{ then } C_1 \text{ else } C_2 \text{ fi} \mid \text{while } p \text{ do } C \text{ od}$$

  where $x \in V$ and $e \in E$ T

- basic commands in C_B:
  1. store assignment
  2. heap lookup
  3. heap mutation
  4. heap allocation
  5. heap deallocation

Predicate Transformers for Basic Commands

notation

we write $[f]$ instead of $[R_f]$ if $f : S_S \to \mathcal{P}\, S_S$ is state transformer

definition

semantic map $[\![-]\!] : C_B \to \mathcal{P}\, S_S \to \mathcal{P}\, S_S$ on basic commands

$$
\begin{aligned}
[\![x := e]\!] &= [\lambda s.\ \{f_a\, x\, e\, s\}] \\
[\![x := *e]\!] &= [\lambda s.\ \{f_l\, x\, e\, s\}] \\
[\![*x := e]\!] &= [\lambda s.\ \{f_m\, x\, e\, s\}] \\
[\![x := \mathsf{alloc}\, e]\!] &= [f_c\, x\, e] \\
[\![\mathsf{dispose}\, e]\!] &= [\lambda s.\ \{f_\ominus\, e\, s\}]
\end{aligned}
$$

Predicate Transformers for Basic Commands

lemma

1. $[\![x := e]\!] = [graph\,(f_a\,x\,e)]$
2. $[\![x := *e]\!] = [graph\,(f_l\,x\,e)]$
3. $[\![*x := e]\!] = [graph\,(f_m\,x\,e)]$
4. $[\![x := \mathsf{alloc}\,e]\!] = [\{(s, s') \mid s' \in f_c\,x\,e\,s\}]$
5. $[\![\mathsf{dispose}\,e]\!] = [graph\,(f_\ominus\,e)]$

. . . in the proper relational semantics

Predicate Transformers for Composite Commands

definition

$[\![-]\!]$ extended to map of type $C \to \mathcal{P}\, S_S \to \mathcal{P}\, S_S$ by

$$
\begin{aligned}
[\![\text{abort}]\!] &= \lambda x.0 \\
[\![\text{skip}]\!] &= id \\
[\![C_1; C_2]\!] &= [\![C_1]\!] \circ [\![C_2]\!] \\
[\![\text{if } p \text{ then } C_1 \text{ else } C_2 \text{ fi}]\!] &= [p] \circ [\![C_1]\!] \cap -[p] \circ [\![C_2]\!] \\
[\![\text{while } p \text{ do } C \text{ od}]\!] &= ([p] \circ [\![C]\!])^{\omega} \circ -[p]
\end{aligned}
$$

Locality in the Concrete Semantics

definition

- set of modified variables in command C

$$\mathsf{MV}\,(x := e) = \mathsf{MV}\,(x := *e) = \mathsf{MV}\,(*x := e) = \mathsf{MV}\,(x := \mathsf{alloc}\,e) = \{x\}$$
$$\mathsf{MV}\,(\mathsf{dispose}\,e) = \mathsf{MV}\,\mathsf{abort} = \mathsf{MV}\,\mathsf{skip} = \emptyset$$
$$\mathsf{MV}\,(C_1; C_2) = \mathsf{MV}\,(\mathsf{if}\ p\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}) = \mathsf{MV}\,C_1 \cup \mathsf{MV}\,C_2$$
$$\mathsf{MV}\,(\mathsf{while}\ p\ \mathsf{do}\ C\ \mathsf{od}) = \mathsf{MV}\,C$$

- set of tests in C

$$\mathsf{T}\,(C_1; C_2) = \mathsf{T}\,C_1 \cup \mathsf{T}\,C_2$$
$$\mathsf{T}\,(\mathsf{if}\ p\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{if}) = \{p\} \cup \mathsf{T}\,C_1 \cup \mathsf{T}\,C_2$$
$$\mathsf{T}\,(\mathsf{while}\ p\ \mathsf{do}\ C\ \mathsf{od}) = \{p\} \cup \mathsf{T}\,C$$
$$\mathsf{T}\,(-) = \emptyset$$

Locality in the Concrete Semantics

lemma

if $C \in C_B$, then

1. $[\![C]\!]$ is isotone
2. $[\![C]\!]$ is p-local if $\mathrm{MV}\ C \cap \mathrm{FV}\ p = \emptyset$

lemma

1. $[\![\mathrm{skip}]\!]$, $[\![\mathrm{abort}]\!]$ are isotone p-local
2. if $[\![C_1]\!]$, $[\![C_2]\!]$ are isotone p-local, then $[\![C_1; C_2]\!]$ is
3. if $[q]$, $[\![C_1]\!]$, $[\![C_2]\!]$ are isotone p-local, then $[\![\mathrm{if}\ q\ \mathrm{then}\ C_1\ \mathrm{else}\ C_2\ \mathrm{fi}]\!]$ is
4. if $[q]$, $[\![C]\!]$ are isotone p-local, then $[\![\mathrm{while}\ p\ \mathrm{do}\ C\ \mathrm{od}]\!]$ is

theorem

If $\mathrm{MV}\ C \cap \mathrm{FV}\ p = \emptyset$ and $\mathrm{T}\ C$ is p-local then $[\![C]\!]$ is p-local

Conclusion

- presented semantics of isotone transformers over complete lattices
- derived PHL and PRC in this setting
- built conjunctive predicate transformers from relational semantics
- introduced notion of p-local transformer over quantale
- showed that PHL and PRC for separation logic derivable in subspace of local isotone transformers
- constructed predicate transformers for store/heap update functions
- related locality with variable conditions on programs/assertions

next lecture: verification conditions for separation logic

Exercises

?

Further Reading

- Back, von Wright, *Refinement Calculus*
- Calcagno et al, *Local Action and Abstract Separation Logic*
- Dongol, Gomes, Struth, *A Program Construction and Verification Tool for Separation Logic*
- Morgan, *Programming from Specifications*
- Rosenthal, *Quantales and Their Applications*